David K. Hemsath
Senior Technical Staff Member, IBM Security Solutions
CISSP, CISSP-ISSAP, CPHIMS, IEEE SM, ACM SM
dhemsath@us.ibm.com

IBM

Cyber security for executives
Nebraska Cyber Security Conference
26 July 2011

Today's discussion topics

- Introduction to Security on a Smarter Planet
- What matters to organizations
- Threats from inside and outside the organization
- Countering the threats: basic cyber security
- How IBM can help

Security on a Smarter Planet

The planet is getting more
Instrumented, **Interconnected** and **Intelligent**.

162 million

Almost 162 million smart phones were sold in 2008, surpassing laptop sales for the first time.

90%

Nearly 90% of innovation in automobiles is related to software and electronics systems.

1 trillion

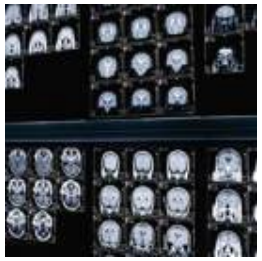
Soon, there will be 1 trillion connected devices in the world, constituting an “internet of things.”

As the world gets smarter, demands on IT are growing:

Smart traffic systems

Intelligent oil field technologies

Smart food systems



Smart healthcare

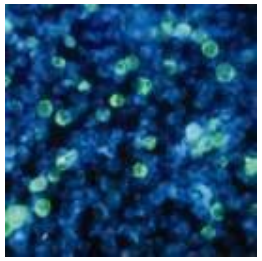
Smart energy grids

Smart retail

Smart water management

Smart supply chains

Smart countries



Smart weather

Smart cities

Smart children

Despite the risk, the reason we will all begin to transform our systems, operations, enterprises and personal lives to take advantage of a smart planet isn't just because we can. **It's because we must.**

Some consequences of this brave new world

- We are seeing a growing convergence between information and operational technologies.
- We are seeing a shift from infrastructure to applications as the preferred attack route.
- Systems have a larger “attack surface” via the Internet, thumb drives, social engineering, policy violations, etc.
- Attacks have moved from the realm of the personal to organized crime and state-sponsored groups.

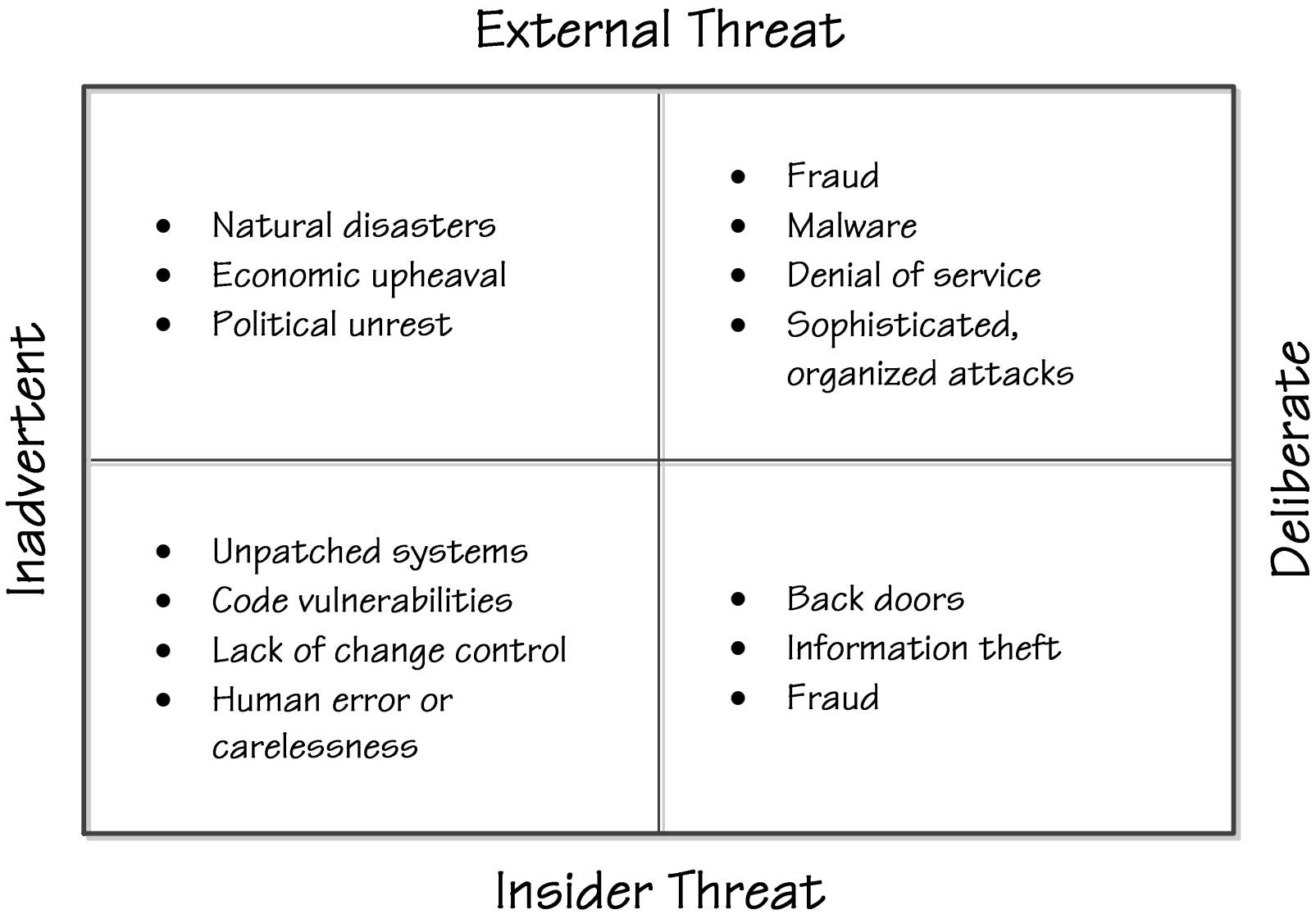
Fundamentally, organizations care about two things

- The continuity of their operations, and
- Protecting sensitive/critical information

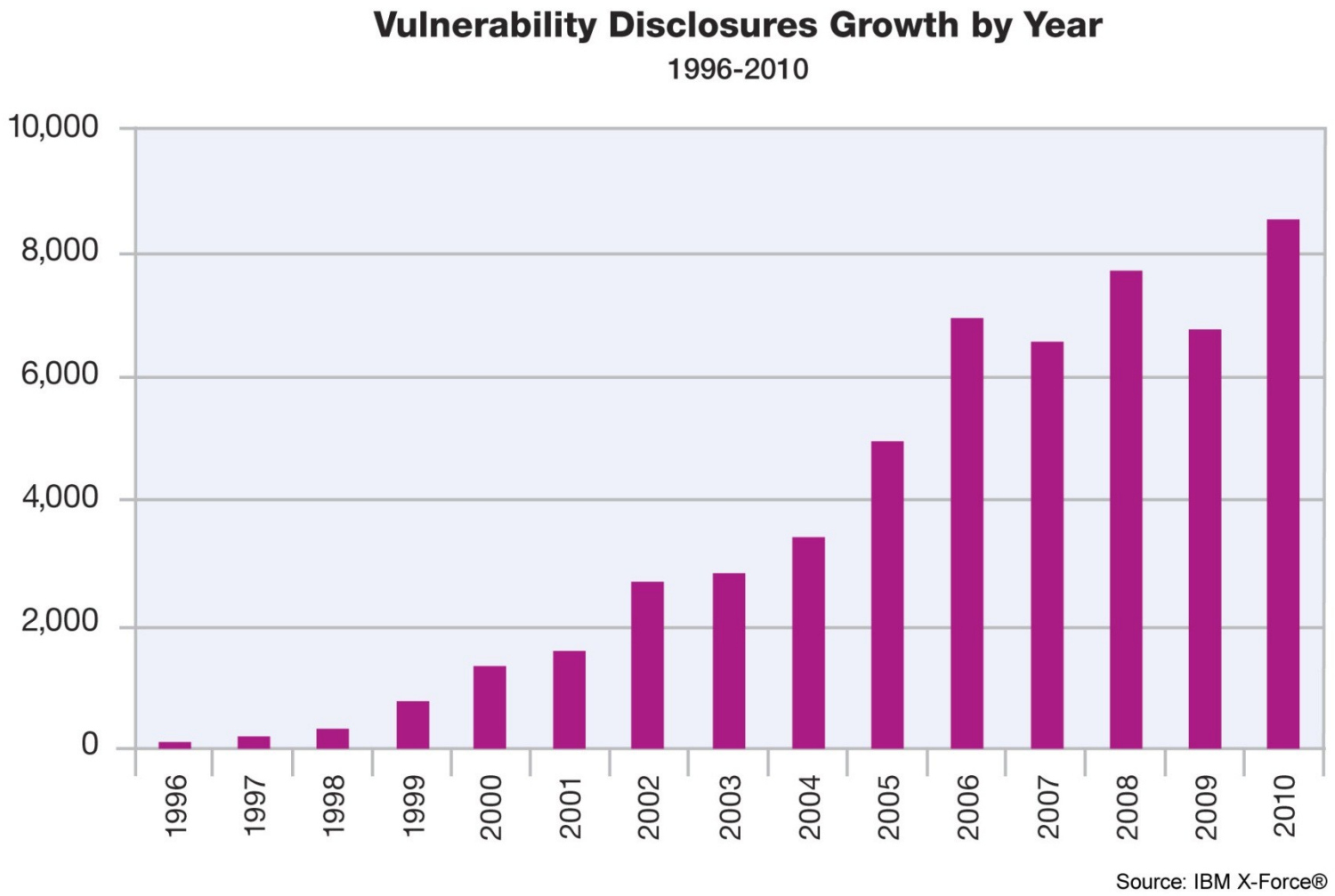
Or, put another way, staying out of the news and staying out of court!

- To achieve this, organizations need to:
  1. Know **who** is coming into their systems,
  2. Know **what** they did, and
  3. Be able to **prove it** to their internal auditors and external regulators.

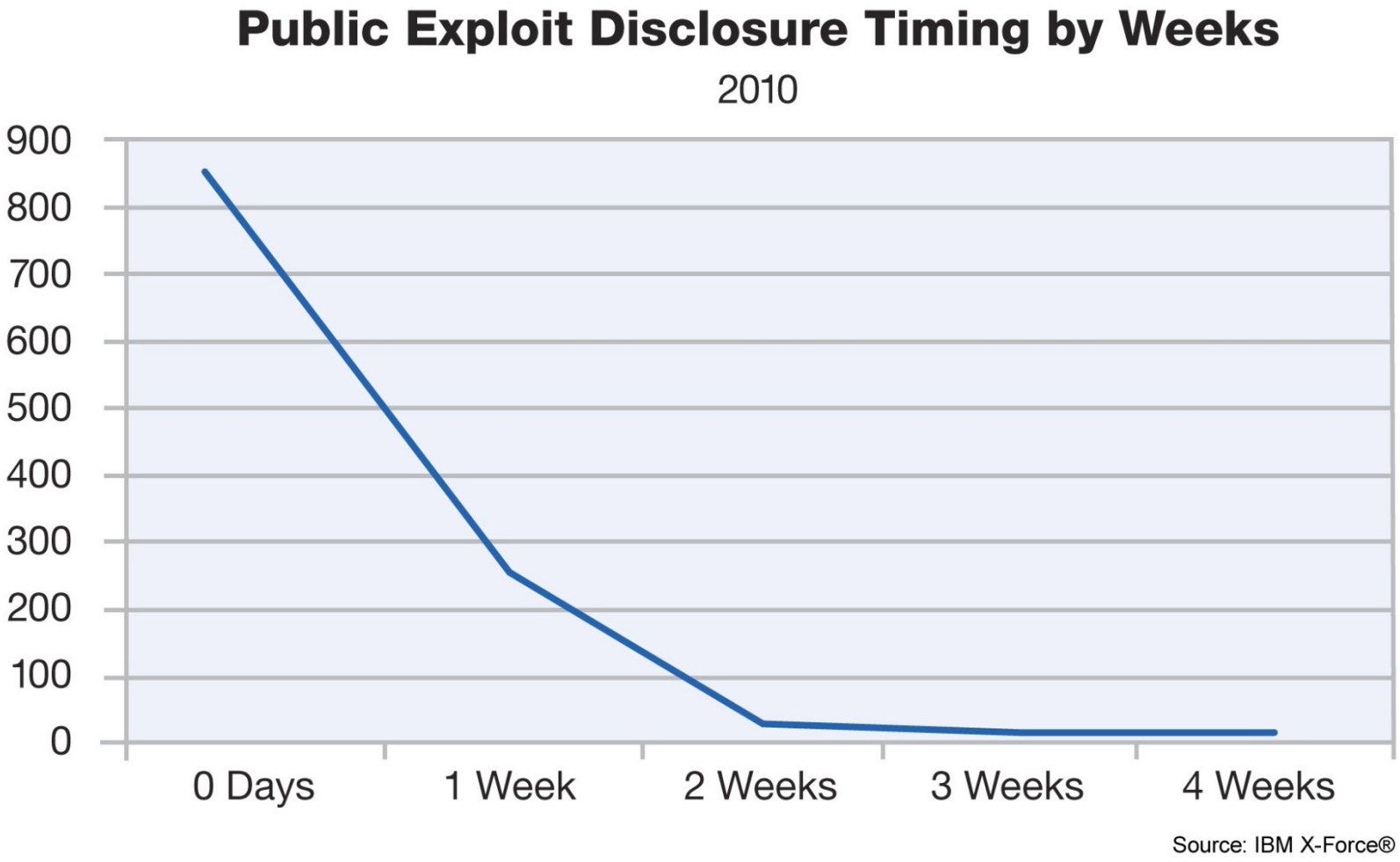
Threats sources



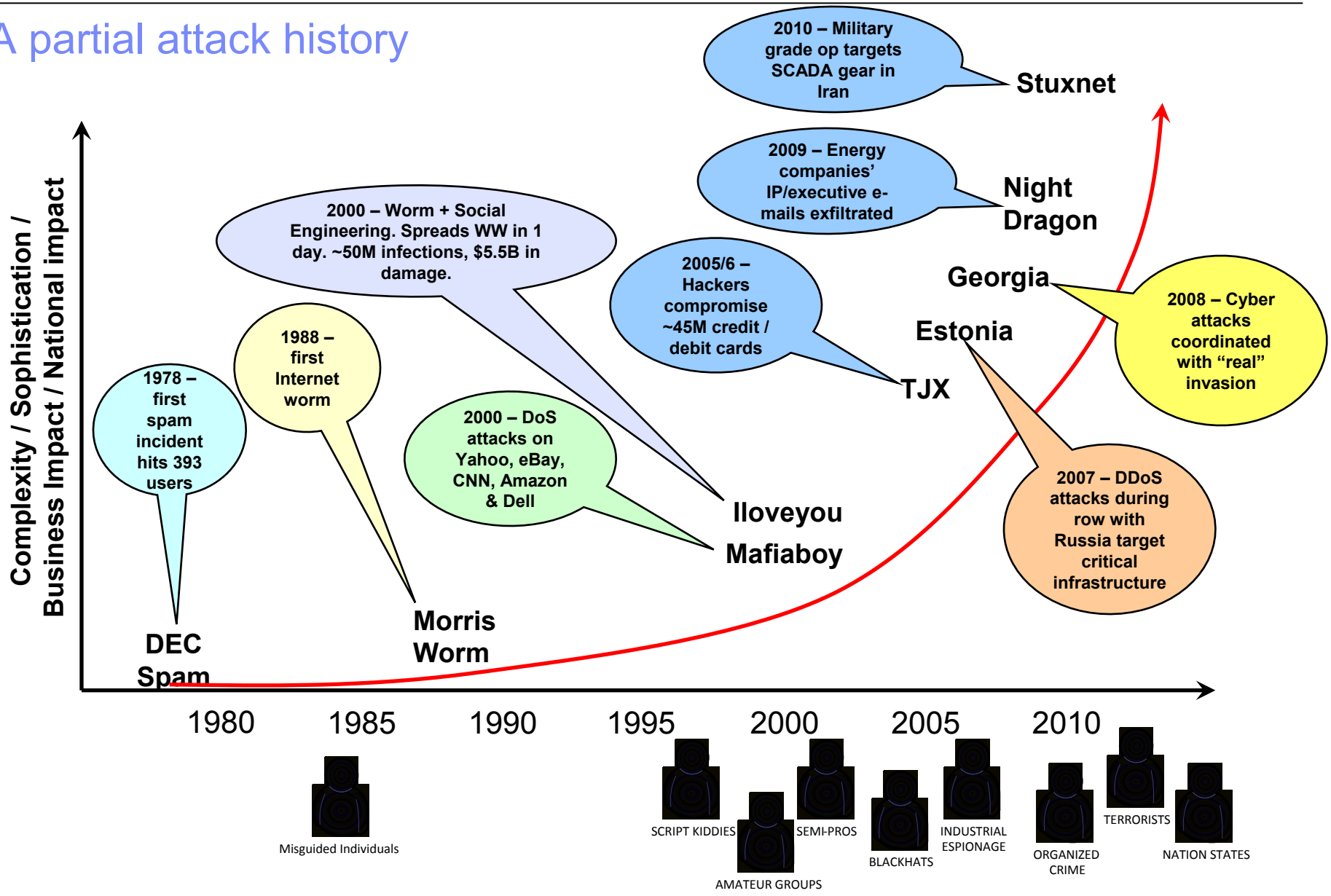
Vulnerabilities continue to be disclosed



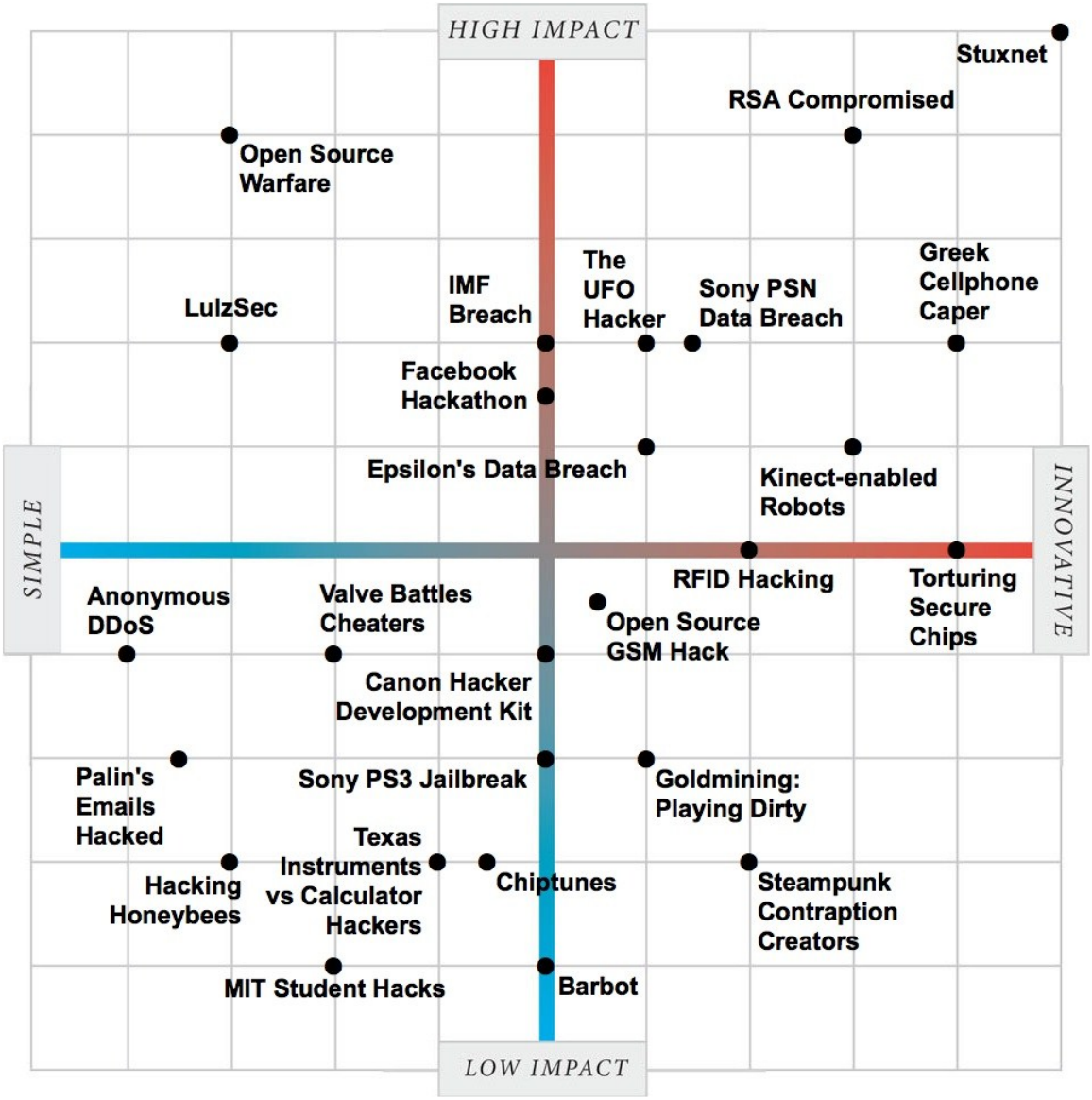
There's usually not much time between a disclosure and an exploit



A partial attack history



More recent attacks
Source: IEEE.org



Cost of data breaches continue to rise (2009 to 2010 data)

- Ponemon Institute "2010 U.S. Cost of a Data Breach" report, published March 2011
  - Direct and indirect cost rose from $204 to $214 per record
    - Does not include reputational damage
  - Average cost of a breach rose from $6.7M to $7.2M
- U.S. Department of Health and Human Services enforcing HIPAA HITECH protected health information rules, e.g.,
  - Massachusetts General Hospital pays $1M due to loss of PHI by hospital employee.
  - University of California at Los Angeles Health System pays $0.865M in HIPAA fines after an investigation found that its employees had been peeking at the electronic personal health information of numerous patients.
- Numerous state breach laws, with possible national breach notification law proposed
- Several recent high-profile data breaches, e.g.,
  - Citigroup,
  - U.S.G.,
  - Sony,
  - …

Insiders remain a problem

- **Rogue trading**
  - October 5, 2010: French trader guilty over Société Générale scandal: Jérôme Kerviel jailed after being found guilty of all charges in trading fraud that cost bank €4.9bn

- **Theft of client records and proprietary trading systems**
  - December 11, 2010: Former Goldman Sachs Programmer Sergey Aleynikov convicted for theft of code from the high-frequency trading system that generates millions of dollars in annual profits

- **Theft of celebrity phone records**
  - September 28, 2010: India's Department of Telecommunications amended telecom licensing rules for national and international long-distance operators, to address security concerns on their networks

- **Viewing of protected health information**
  - January 12, 2011: TUCSON - Three University Medical Center workers were fired this week for accessing confidential medical records, a patient privacy violation.

One attack scenario: outsiders exploit insiders*

1. Criminals target someone in your organization

Targeting occurs via Phishing, Spear Phishing, and Social Engineering. Malware is introduced via infected attachment in an email or thumb drive, or by directing your user to click on a malicious link. Malware can include keystroke logging and screen shot functions.

2. Malware is installed

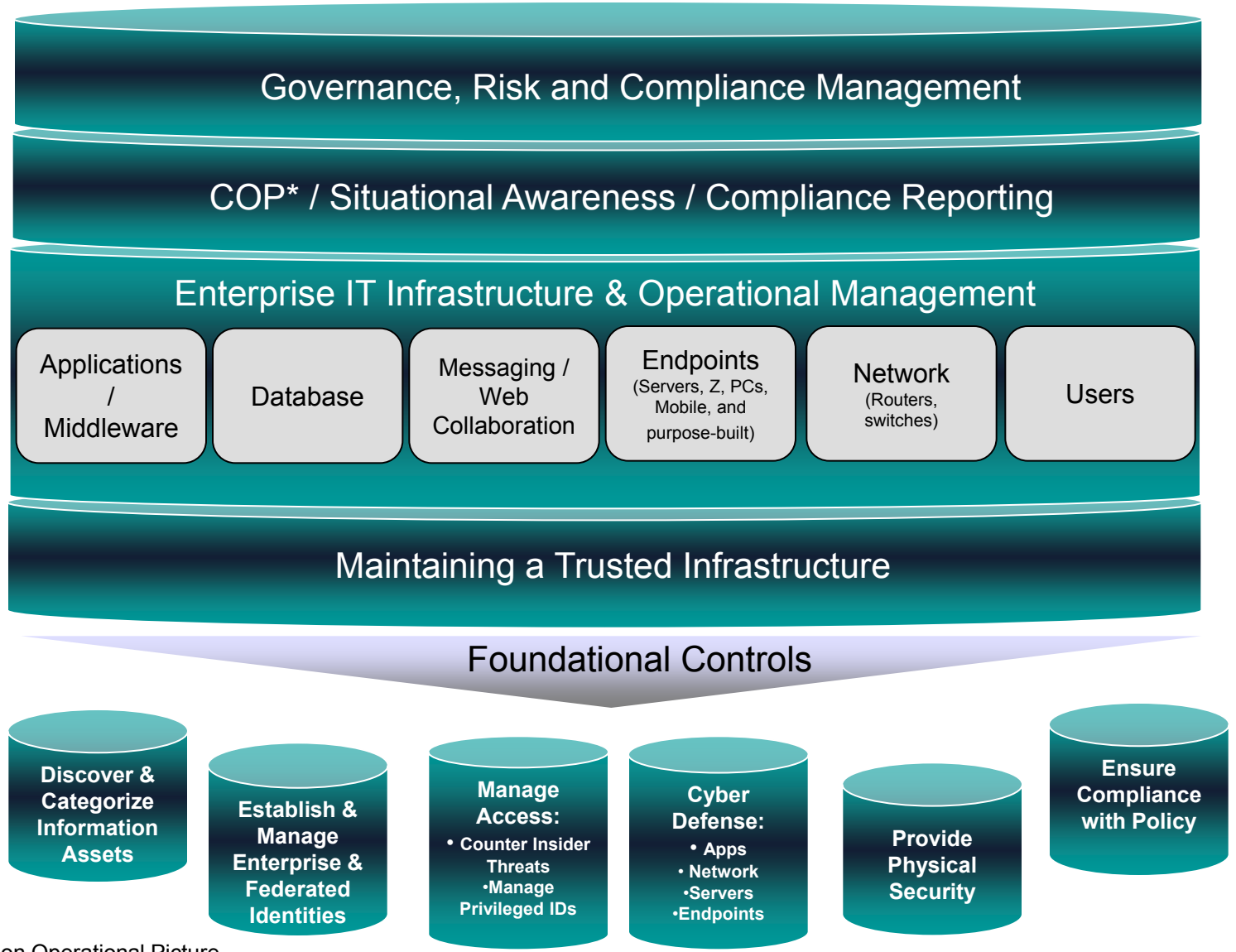
3. Victim logs on to company's internet banking account

4. Malware collects and transmits account #s and passwords

5. Criminals use stolen internet banking credentials to initiate funds transfer

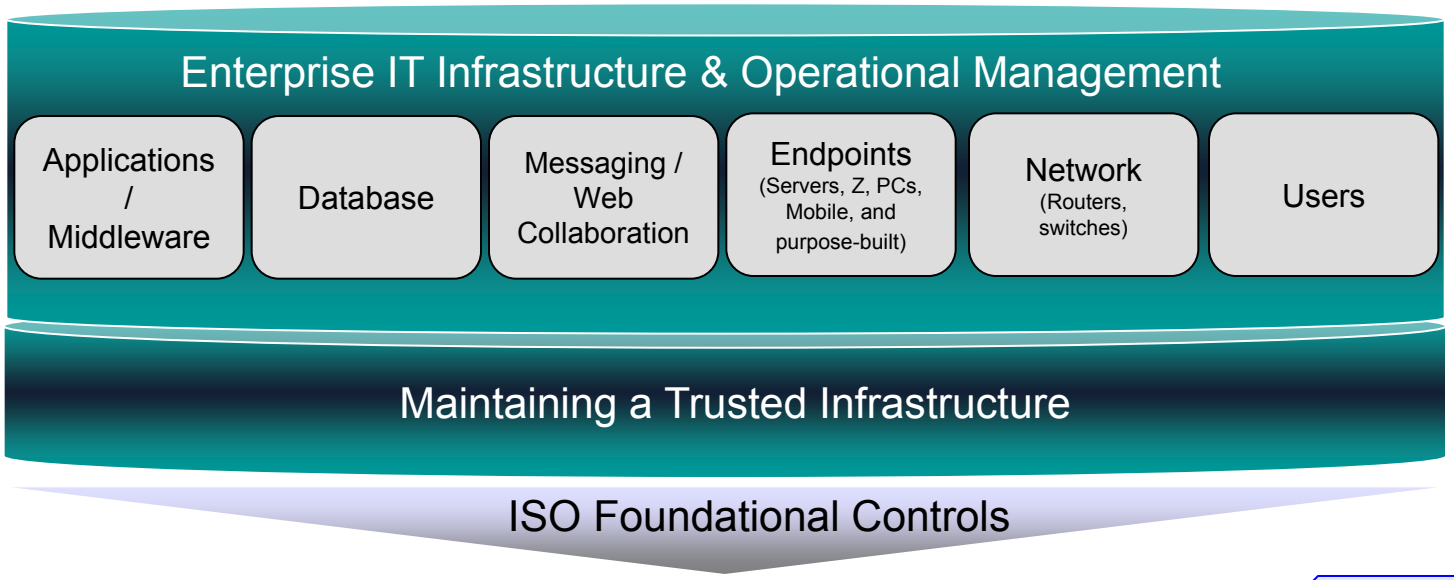
*Note: the same basic approach is used to steal other assets.

Countering the threats: foundational cybersecurity



* Common Operational Picture

Another view: standards-based maturity models



ISO Foundational Controls

Risk Assessment & Treatment

Security Policy

Organization of Information Security

Asset Management

Human Resources Security

Physical / Environmental Security

Comm & Ops Management

Access Management

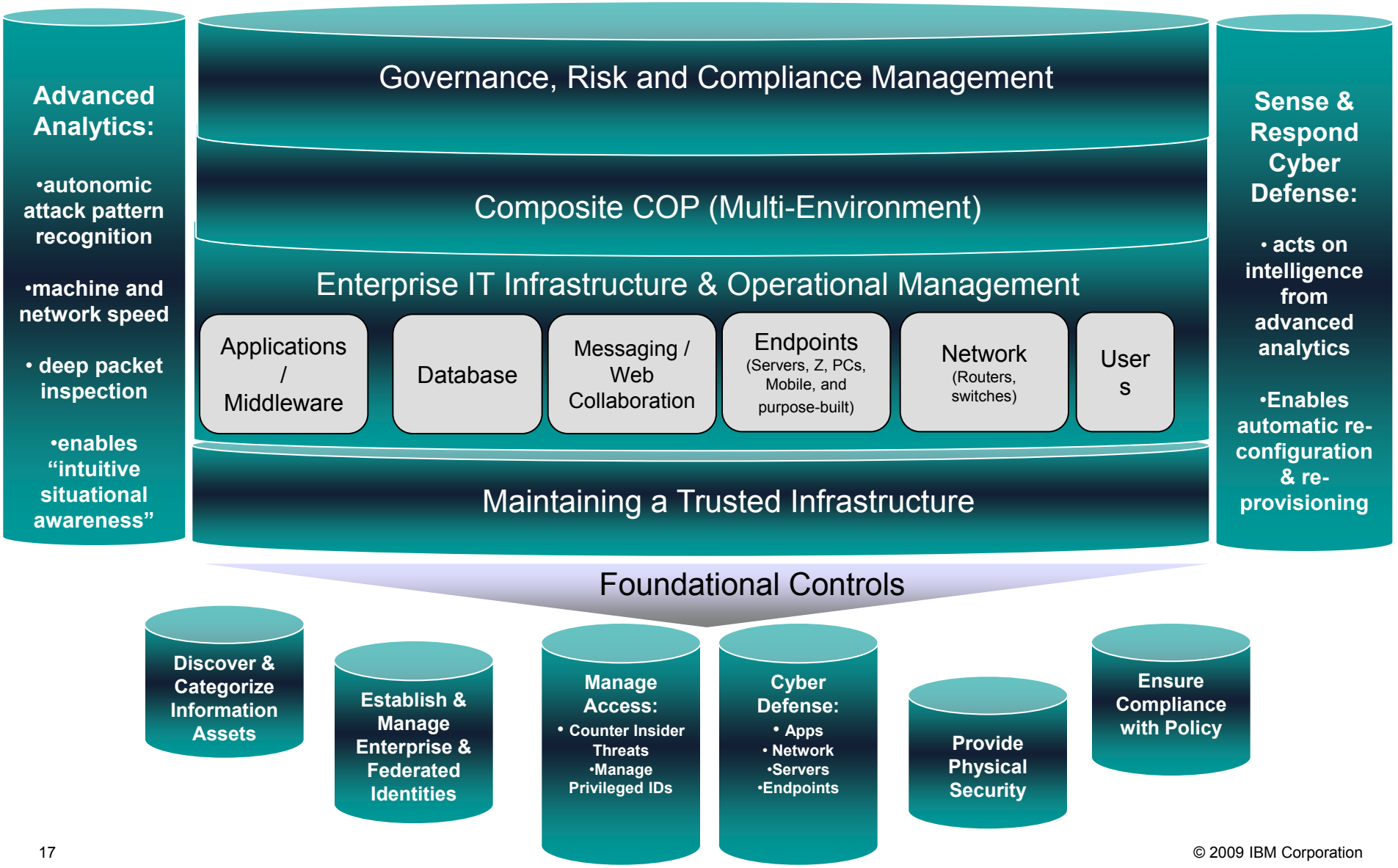
Acquisition, Development & Maintenance

Incident Management

Business Continuity

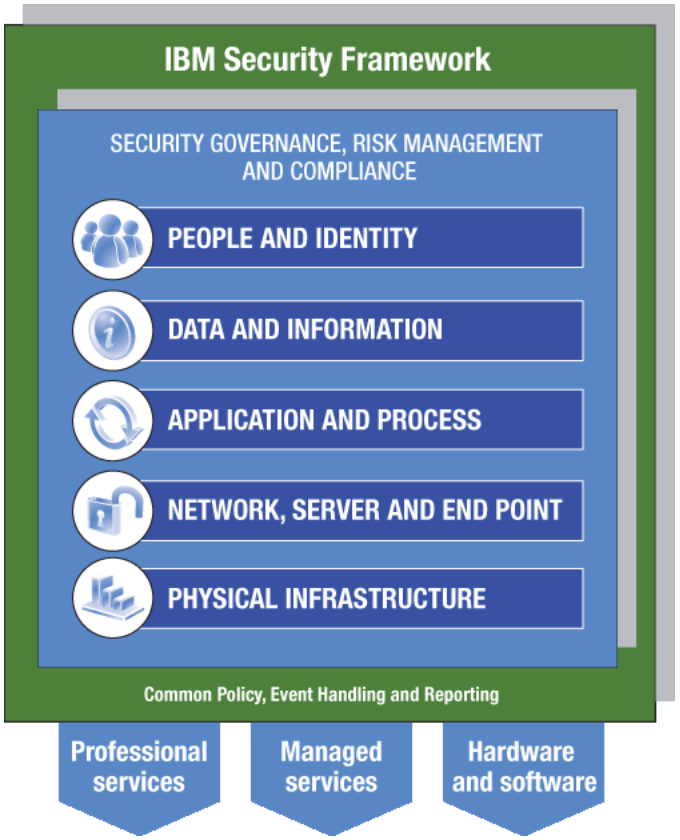
Compliance

The future: automating security & resilience



How can IBM help?

- Standards-based approaches
- Commercially available solutions for
  - Information discovery
  - Cyber security
  - Business continuity & resiliency
  - Asset management
  - Integrated, automated service management for cloud
  - Advanced analytics
- Security evaluations:
  - Common Criteria
  - CMVP
- Extensive experience with our own operation
- Extensive experience managing security for clients
  - Managed Security Services (3,700+ clients)
  - Strategic Outsourcing Clients



The Importance of Research to Security: IBM Internet Security Systems X-Force® Research Team

Research → Technology → Solutions

- Original Vulnerability Research
- Public Vulnerability Analysis
- Malware Analysis
- Threat Landscape Forecasting
- Protection Technology Research

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

The X-Force team delivers reduced operational complexity – helping to build integrated technologies that feature "baked-in" simplification- "Protecting people from themselves"

Resources

- www.ibm.com/security
- IBM Redguide: Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security
- IBM Redguide: Security in Development: The IBM Secure Engineering Framework
- IBM Redbook: IBM Security Solutions Architecture for Network, Server and Endpoint
- IBM X-Force® 2010 Trend and Risk Report
- *Cyber War*, by Richard A. Clarke
- The IT Industry's Cybersecurity Principles for Industry and Government